# Cryptanalysis of Lee-Hwang-Li's Key Authentication Scheme

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{zhfg, kkj}@icu.ac.kr

**Abstract.** Key authentication is very important in secret communications and data security. Recently, Lee, Hwang and Li proposed a new public key authentication scheme for cryptosystems with a trusty server. However, in this paper, we will show that Lee-Hwang-Li's key authentication scheme is not secure, from the obtained public information, any one can get the private key of the user. And then, we propose an improved scheme. We conclude that our new key authentication scheme not only resolves the problems appeared but also is secure.

**Key words:** Key authentication scheme, Cryptanalysis, Certificate, Password.

## 1 Introduction

The public key cryptography was introduced by Diffie and Hellman in 1976 [1], in such cryptosystem, each user has two keys: a public key and a private key. There is a possible danger event in public key cryptosystem: an intruder can revise the public key from the public-key directory and substitute the public key of a target user. In this way, the intruder can impersonate the public key of this target user and, hence, raise a security threat of fabrication. The purpose of key authentication is to verify the public key of a legal user and prevent a forged public key. Therefore, key authentication is very important in secret communications and data security.

Many key authentication schemes have been proposed. In 1996, Horng and Yang [2] proposed a key authentication scheme based on the discrete logarithm problem, but three years later, Zhan *et al.* [7] pointed out that Horng-Yang's scheme couldn't prevent from the guessing attack [5] and gave an improved scheme. In [4], Lee, Hwang and Li showed that Zhan *et al.*'s improved scheme didn't achieve non-repudiation of user's public key (*i.e.*, a dishonest legal user can deny his public key), and proposed a new public key authentication scheme for cryptosystems with a trusty server. Their scheme is based on discrete logarithm too, and in their scheme, the certificate of the public key is a combination of user's password and private key. The authors declared that their scheme was secure for the others public key authentication. However, in this paper, we shall show that Lee-Hwang-Li's key authentication scheme is not secure, from the obtained public information, any one can get the private key of the user. And then, we propose an improved scheme. Through our analysis, our new key authentication scheme not only resolves the problems appeared but also is secure.

The organization of this paper is as follows: In Section 2 we describe Lee-Hwang-Li's key authentication scheme, and in Section 3, we propose an attack on this scheme. We propose a new key authentication scheme in Section 4, in Section 5 we give an analysis of our new scheme. We make a concluding remark in the final section.

## 2 Lee-Hwang-Li Key Authentication Scheme

First of all, we review Lee-Hwang-Li key authentication scheme in brief using the same notation as [4].

The user of the system has **Prv** as his/her private key and **PWD** as his/her password. Let **Pub** of the user's public key be

$$\mathbf{Pub} = g^{\mathbf{Prv}} \bmod p$$

where $p$ is a large prime, $g$ is a generator in $Z_p^*$. The $p, g$ and one-way function $f : f(x) = g^x \bmod p$ are public parameters.

In the user's registration phase, each user chooses a random number $r \in Z_p^*$ such that $\gcd((\mathbf{PWD} + r), \mathbf{Prv}) = 1$, and then calculates $f(\mathbf{PWD} + r)$. When $\gcd((\mathbf{PWD} + r), \mathbf{Prv}) = 1$, we can find two integers $a$ and $b$ such that the following equation holds:

$$a(\mathbf{PWD} + r) + b\mathbf{Prv} = 1.$$

The user then sends $f(\mathbf{PWD}+r)$, $R = g^r \bmod p$, $a$ and $b$ to the server secretly. $f(\mathbf{PWD} + r)$, $a$ and $b$ are stored in public password table in the server. The public password table cannot modify or forge by an attacker because the server can use the technique access control to protect it. The server then verifies if $f(\mathbf{PWD}+r) = f(\mathbf{PWD}) \times R$ and then verifies if $f(\mathbf{PWD})^a \cdot \mathbf{Pub}^b = g \bmod p$. If the equations are equal, the server then verifies the $f(\mathbf{PWD}+r)$, $a$ and $b$ sent by the legal user. The certificate $C$ of user's public key is as follows:

$$C = \frac{(\mathbf{PWD} + r)}{f(\mathbf{PWD} + r) + \mathbf{Prv}} \bmod (p - 1).$$

The certificate $C$ and public-key **Pub** of the user are opened to the public over the network. The $f(\mathbf{PWD} + r)$, $a$ and $b$ are opened to the public in the server that protected by the server using access control.

In the key authentication phase, when someone wants to communicate with a user, the sender first obtains $C$, **Pub**, $a$, $b$ and $f(\mathbf{PWD} + r)$ of the receiver from the public directory in the network and public password table in the server, and then checks the certificate $C$ of the public key of the receiver by computing the following equation:

$$\begin{aligned} f(C) &= f(\mathbf{PWD}+r)^{a\times C} \times \mathbf{Pub}^{b\times C} \bmod p \\ &= g^{a\times(\mathbf{PWD}+r)\times C} \times g^{b\times\mathbf{Prv}\times C} \bmod p \\ &= g^{a\times(\mathbf{PWD}+r)\times C+b\times\mathbf{Prv}\times C} \bmod p \\ &= g^{C\times(a\times(\mathbf{PWD}+r)+b\times\mathbf{Prv}} \bmod p \\ &= g^{C} \bmod p \end{aligned}$$

If the above equation holds, the sender accepts the public-key **Pub** of the receiver to encrypt the transmission message, otherwise, the sender rejects the **Pub** of the receiver.

## 3 An Attack on Lee-Hwang-Li Scheme

In this section, we propose an attack on Lee-Hwang-Li's key authentication scheme. By our attack, any one can recover the private key of any user in their system. The details of our attack are described as follows:

For any one, say Alice, can obtain some public information $C$, **Pub**, $a$, $b$ and $f(\mathbf{PWD}+r)$ of any user from the public directory in the network and public password table in the server. We know that

$$C = \frac{(\mathbf{PWD}+r)}{f(\mathbf{PWD}+r)+\mathbf{Prv}} \bmod (p-1)$$

So we have

$$C \times (f(\mathbf{PWD}+r)+\mathbf{Prv}) = (\mathbf{PWD}+r) \bmod (p-1),$$

*i.e.*,

$$\mathbf{Prv} = C^{-1} \times (\mathbf{PWD}+r) - f(\mathbf{PWD}+r) \bmod (p-1). \qquad (1)$$

On the other hand, we have

$$a(\mathbf{PWD}+r) + b\mathbf{Prv} = 1.$$

So,

$$a(\mathbf{PWD}+r) + b\mathbf{Prv} = 1 \bmod (p-1). \qquad (2)$$

From Eqs (1) and (2), any one can solve the unique solution **Prv** and $(\mathbf{PWD}+r)$ in $[0, p-1]$, and we know $\mathbf{Prv} \in [0, p-1]$. More precisely, we can get:

$$(\mathbf{PWD}+r) = (a+bC^{-1})^{-1}(1+bf(\mathbf{PWD}+r)) \bmod (p-1)$$

$$\mathbf{Prv} = C^{-1} \times (a+bC^{-1})^{-1}(1+bf(\mathbf{PWD}+r)) - f(\mathbf{PWD}+r) \bmod (p-1).$$

From above, any one can recover the private key of any user in Lee-Hwang-Li's key authentication scheme. So the security of their scheme does not rely on the discrete logarithm problem as they claimed.

## 4 Improved Scheme

In this section, we propose an improved key authentication scheme.

The system parameters of our key authentication scheme are as follows: Let $p$ and $q$ be prime numbers such that $q|p-1$, $g$ is a generator with order $q$ in $Z_p^*$. The one-way function $f$ is defined by $f(x) = g^x \bmod p$. The user of the system has **Prv** as his/her private key and **PWD** as his/her password. Let **Pub** of the user's public key is

$$\mathbf{Pub} = g^{\mathbf{Prv}} \bmod p.$$

In the user's registration phase, the certificate of the public key of the user is generated by the user with his/her password and private key. Each user chooses a random number $r \in Z_q^*$, and then calculates $f(\mathbf{PWD} + r)$. The certificate $C$ of user's public key is as follows:

$$C = \mathbf{PWD} + r + \mathbf{Prv} \cdot \mathbf{Pub} \bmod q.$$

The user then sends $f(\mathbf{PWD} + r)$, $R = g^r \bmod p$ and his ID to the server secretly. The server then verifies if $f(\mathbf{PWD} + r) = f(\mathbf{PWD}) \times R$ and verifies the $f(\mathbf{PWD} + r)$ sent by the legal user, and then stores ID and $f(\mathbf{PWD} + r)$ in public password table in the server. The public password table cannot modify or forge by an attacker because the server can use the technique access control to protect it. The certificate $C$ and public-key **Pub** of the user are opened to the public over the network.

In the key authentication phase, when someone wants to communicate with a user, the sender first obtains $C$, **Pub** and $f(\mathbf{PWD} + r)$ of the receiver from the public directory in the network and public password table in the server, and then checks the certificate $C$ of the public key of the receiver by computing the following equation:

$$f(C) = f(\mathbf{PWD} + r) \times \mathbf{Pub}^{\mathbf{Pub}} \bmod p.$$

If the above equation holds, the sender accepts the public-key **Pub** of the receiver to encrypt the transmission message, otherwise, the sender rejects the **Pub** of the receiver.

The Elliptic Curve Cryptosystem (ECC) [3, 6] provides the high security per bit and greater efficiency over other public key systems known today. Our new key authentication scheme can be straightforwardly constructed using ECC. In ECC version, the certificate $C$ can be constructed as follows:

$$C = \mathbf{PWD} + r + \mathbf{Prv} \cdot R_x(\mathbf{Pub}) \bmod q,$$

and the verification will be:

$$f(C) = f(\mathbf{PWD} + r) + R_x(\mathbf{Pub}) \cdot \mathbf{Pub}.$$

Here the one-way function $f$ is defined by $f(\lambda) = \lambda P$, and $P$ is a generator with order $q$ in elliptic curve $E_{(a,b)} : y^2 = x^3 + ax + b$ over finite field $F_p$, $R_x(A)$ denotes the $x$-coordinate of point $A$.

## 5 Analysis of the New Scheme

Our scheme provides verification of a user's public key. Preventing the impersonation of a public key is managed through the difficulty of discrete logarithm problem. If an intruder attempts to forge a user's public key, suppose that he/she wants to substitute a false key $\mathbf{Pub_{false}}$ for a user's public key, then the false certificate $C_{false}$ should satisfy the key authentication equation:

$$f(C_{false}) = f(\mathbf{PWD} + r) \times \mathbf{Pub_{false}^{Pub_{false}}} \bmod p.$$

To find $C_{false}$, the intruder has to compute

$$C_{false} = f^{-1}(f(\mathbf{PWD} + r) \times \mathbf{Pub_{false}^{Pub_{false}}} \bmod q.$$

This is impossible, since the intruder has to solve the discrete logarithm problem. If the intruder can obtain the user's $\mathbf{PWD}$ and $r$ or can forge $f(\mathbf{PWD} + r)$, then he/she can get the false certificate $C_{false}$ from

$$C_{false} = (\mathbf{PWD} + r) \times \mathbf{Prv_{false}^{Pub_{false}}} \bmod q.$$

This is impossible too. The intruder cannot modify and forge $f(\mathbf{PWD} + r)$ because the public password table is protected by the server using the access control.

In Horng-Yang's scheme [2], an intruder can guess the user's **PWD** using the guessing attack [5]. Then he/she can obtain the users private key. Thus, an intruder can forge the users public key. In our scheme, if an intruder attempts to forge the users public key, he/she must simultaneously guess $r$ and **PWD**. This is difficult because $r \in Z_q$ is a very long random number. Therefore, an intruder cannot use the guessing attack in our scheme to forge the users public key.

Now we show that our scheme can achieve non-repudiation of the users public key. Suppose that there is a dishonest user having a pair of public-private keys (**Pub**, **Prv**). After he/she signed a document using his/her private key **Prv**, then anyone can verify this signature using **Pub**, but this dishonest user wants to deny this signature, then he/she must show that he/she has another public key **Pub'** and certificate $C'$, and they passed the key authentication phase, *i.e.*,

$$f(C') = f(\mathbf{PWD} + r) \times \mathbf{Pub'^{Pub'}} \bmod p.$$

But he/she cannot derive another **Pub'** and $C'$ even he/she knows $f(\mathbf{PWD}+r)$. Since the dishonest user only can do as follows: (1), he/she can forge a public key **Pub'**, and then to get the certificate $C'$ from $f(\mathbf{PWD}+r) \times \mathbf{Pub'^{Pub'}}$, this is to solve the discrete logarithm problem. (2), he/she can first forge a certificate $C'$, and then to find **Pub'**, such that $\mathbf{Pub'^{Pub'}} = f(C') \times f(\mathbf{PWD} + r)^{-1}$, this is to solve the equation: $x^x = A \bmod p$. So, we say that our key authentication scheme can achieve non-repudiation of the user's public key.

## 6 Conclusion

In this paper, we have shown that Lee-Hwang-Li's key authentication scheme is not secure, from the obtained public information, any one can get the private key of the user. And then, we proposed an improved scheme, also we gave a ECC version of our new scheme. We conclude that our new key authentication scheme not only withstands the guessing attack but also achieves non-repudiation of the user's public key.

## References

1. W. Diffie and M. E. Hellman, *New Directions in Cryptography*, IEEE Trans. on Information Theory, 22, pp.644-654, 1976.
2. G. Horng and C.S. Yang, *Key authentication scheme for cryptosystems based on discrete logarithms*, Computer Communications, 19 (1996) 848-850.
3. N. Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation,48, pp.203-209, 1987.
4. C-C. Lee, M-S. Hwang and L-H. Li, *A new key authentication scheme based on discrete logarithms*, Applied Mathematics and Computation 139 (2003), pp.343-349.
5. G. Li, M.A. Lomas, R.M. Needham, J.H. Saltzer, *Protecting poorly chosen secrets from guessing attacks*, IEEE Journal on Selected Areas in Communications 11 (1993) 648?56.
6. V.S. Miller, *Use of Elliptic Curve in Cryptography*, In Advances in Cryptology-CRYPTO'85, LNCS.218, Spring-Verlag, pp.417-426, 1986.
7. B. Zhan, Z. Li, Y. Yang, Z. Hu, *On the security of HY-key authentication scheme*, Computer Communications 22 (1999) 739- 741.